

4-Port ADSL Router

Lynx L-325

User Manual

Version 1.0

Version Date: July 8, 2005
Document #: BD-AU0007-10

Table of Contents

GENERAL INFORMATION	3
<i>Package Contents</i>	3
<i>Safety Instructions—Please read.</i>	3
<i>Front Panel View</i>	4
<i>Back Panel View</i>	5
INSTALLING THE ROUTER	6
<i>Connect the ADSL Line and Telephone</i>	6
<i>Connect the PC to the Router</i>	6
<i>Connect the Power Adapter</i>	6

INSTALLATION DIAGRAM	7
CONFIGURING YOUR COMPUTER	8
<i>Windows 2000</i>	8
<i>Windows XP</i>	9
LOG IN TO THE ROUTER.....	10
DEVICE INFO.....	11
<i>Summary</i>	11
<i>WAN</i>	11
<i>STATISTICS</i>	12
LAN Statistics	12
WAN Statistics.....	12
ATM Statistics.....	13
ADSL Statistics.....	13
ADSL BER Test.....	15
<i>Route</i>	17
<i>ARP</i>	17
QUICK SETUP	18
<i>ATM PVC Configuration</i>	18
ADVANCED SETUP	22
<i>WAN</i>	22
Connection Type	24
<i>NAT</i>	27
Virtual Servers	27
Port Triggering.....	29
DMZ Host	30
<i>Firewall</i>	31
IP Filtering—Outgoing.....	31
IP Filtering—Incoming.....	32
MAC Filtering.....	33
<i>Port Mapping</i>	34
<i>Quality of Service</i>	36
<i>Routing</i>	37
Default Gateway	37
Static Route	38
RIP.....	39
<i>DNS</i>	39
DNS Server	39
Dynamic DNS	40
<i>ADSL</i>	41
DSL Advanced Settings.....	42
Tone Settings	43
DIAGNOSTICS	44
MANAGEMENT	45
<i>Settings</i>	45
Backup Settings.....	45

Restore User Settings	46
Restore Default.....	46
<i>System Log</i>	47
Configure System Log	48
<i>SNMP</i>	48
<i>Internet Times</i>	49
<i>Access Control</i>	51
Services.....	51
IP Addresses	51
Passwords.....	52
<i>Update Software</i>	53
<i>Reboot Router</i>	53

General Information

The 4-Port ADSL Router features 4 LAN ports for added convenience and accessibility.

Package Contents

Included in the package is one of each of the following—

- 4-Port ADSL router
- 15 VAC AC power adapter
- RJ-11 telephone cable
- RJ-45 Ethernet cable
- Splitter
- User Manual



Safety Instructions—Please read.

- Place your router on a flat surface close to the cables in a location with sufficient ventilation.
- To prevent overheating, do not obstruct the ventilation openings of this equipment.
- Plug this equipment into a surge protector to reduce the risk of damage from power surges and lightning strikes.
- Operate this equipment only from an electrical outlet with the correct power source as indicated on the adapter.
- Do not open the cover of this equipment. Opening the cover will void any warranties on the equipment.
- Unplug equipment first before cleaning. A damp cloth can be used to clean the equipment. Do not use liquid / aerosol cleaners or magnetic / static cleaning devices.

Front Panel View



LED	Mode	Indication
DSL	Solid	ADSL is connected.
	No light	ADSL is not connected.
	Blinking	The router is connected to ADSL.
ETH1-ETH4	Solid	Router is connected to the LAN.
	No light	No connection to the LAN. Check if the LAN cable is connected to the router.
	Blinking	LAN traffic
INT	Solid	PPP user ID accepted
	No light	PPP not connected
POWER	Solid	Router is powered on.
	No light	Router is not powered. Check if the router is plugged in and if the power switch is turned on.

Back Panel View

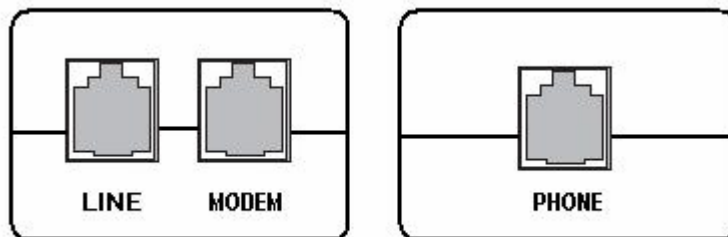


Port	Description
Power Switch	Press to turn the router on and off.
Power	Connects to a 15 VAC AC power adapter.
Reset	Restart —press the button for less than 4 seconds. Default settings —press the button for 4 seconds or longer.
LAN1-LAN4	RJ-45 connects the unit to an Ethernet device such as a PC or a switch.
Line	ADSL connection.

Installing the Router

Connect the ADSL Line and Telephone

An RJ-11 cable will be connected to the wall phone jack and the line-end of the splitter. Connect another RJ-11 phone cable from the modem-end of the splitter to the port labeled “line” on the router. A third RJ-11 phone cable will be needed to connect the telephone to the phone-end of the splitter.



NOTE: See connections on the installation diagram.

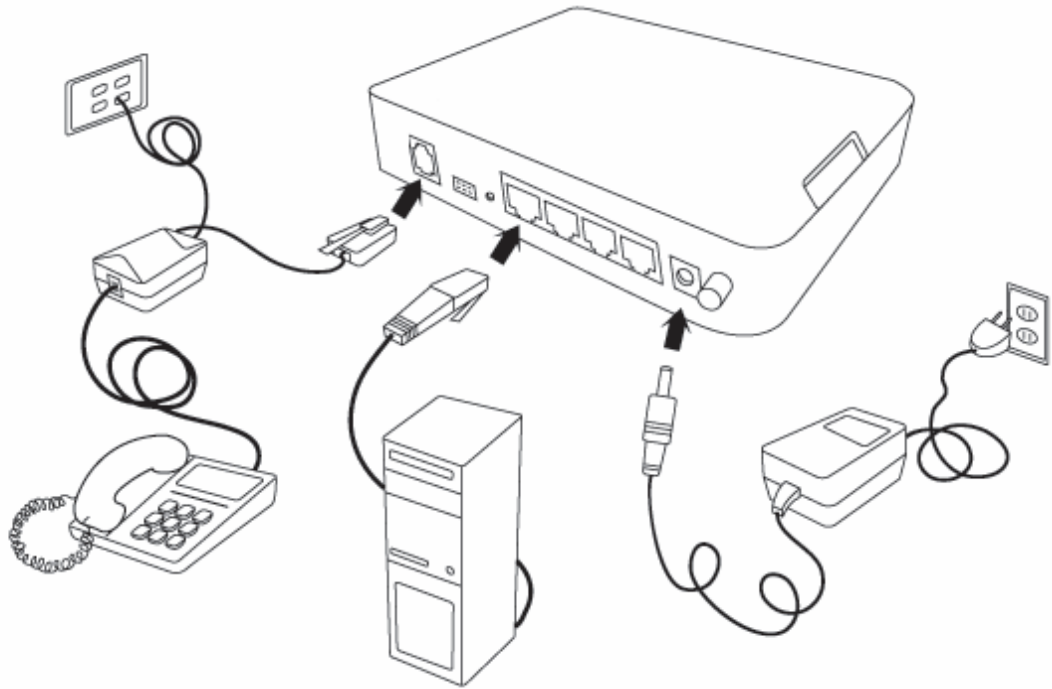
Connect the PC to the Router

Use the Ethernet cable to connect your computer directly to the router. Connect one end of the Ethernet cable to one of the ports labeled LAN on the rear panel of the router and connect the other end to the Ethernet port of your computer. Attach any additional PCs to the router using RJ-45 cables to the port labeled LAN on the rear panel of the router.

Connect the Power Adapter

Complete the process by connecting the AC power adapter to the POWER connector on the back of the device and plug the adapter into a wall outlet or power strip. Then turn on and boot up your PC and any LAN devices, such as hubs or switches, and any computers connected to them.

Installation Diagram



Configuring Your Computer

Prior to accessing the router through the LAN port, note the following necessary configurations—

- Your PC's TCP/IP address: **192.168.1.__(** the last number is any number between 3 and 254)
- The router's default IP address: **192.168.1.1**
- Subnet mask: **255.255.255.0**

Below are the procedures for configuring your computer. Follow the instructions for the operating system that you are using.

Windows 2000

1. In the Windows taskbar, click on the Start button and point to Settings, Control Panel, and Network and Dial-up Connections (in that order).
2. Click on Local Area Connection. When you have the Local Area Connection Status window open, click on **Properties**.
3. Listed in the window are the installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled, and you can skip to Step 10.
4. If Internet Protocol (TCP/IP) does not appear as an installed component, then click on **Install**.
5. In the Select Network Component Type window, click on protocol and then the **Add** button.
6. Select Internet Protocol (TCP/IP) from the list and then click on **OK**.
7. If prompted to restart your computer with the new settings, click **OK**.

8. After your computer restarts, click on the Network and Dial-up Connections icon again, and right click on the Local Area Connection icon and then select Properties.
9. In the Local Area Connection Properties dialog box, select Internet Protocol (TCP/IP) and then click on **Properties**.
10. In the Internet Protocol (TCP/IP) Properties dialog box, click in the radio button labeled **Use the following IP address** and type 192.168.1.x (where x is any number between 2 and 254) and 255.255.255.0 in the IP address field and Subnet Mask field.
11. Click on **OK** twice to save your changes and then close the **Control Panel**.

Windows XP

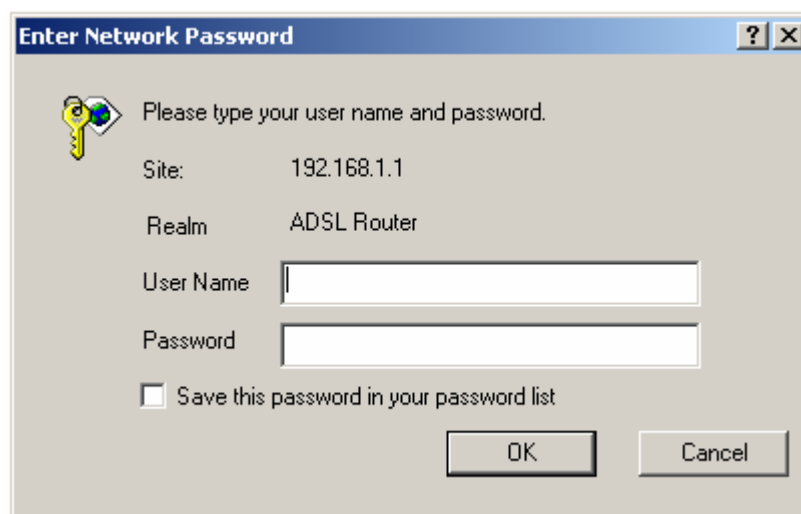
1. In the Windows taskbar, click on the Start button and point to Settings and then click Network Connections.
2. In the Network Connections window, right click on the Local Area Connection icon and click on properties.
3. Listed in the Local Area Connection window are the installed network components. Make sure the box for Internet Protocol (TCP/IP) is checked and then click on **Properties**.
4. In the Internet Protocol (TCP/IP) Properties dialog box, click in the radio button labeled **Use the following IP address** and type 192.168.1.x (where x is any number between 2 and 254) and 255.255.255.0 in the IP address field and Subnet Mask field.
5. Click on **OK** twice to save your changes and then close the **Control Panel**.

Log in to the Router


This section explains how to log in to your router using the following steps—

1. Launch your web browser.
2. Enter the URL <http://192.168.1.1> in the address bar and click on **Enter**.

A login screen like the one below will be displayed after you connect to the user interface.



3. Enter your user name and password, and then click on **OK** to display the user interface.

 **NOTE:** *There are two default user name and password combinations. The user / user combination can display device status, but cannot change or save configurations and are limited to only certain screens. The admin / admin combination can perform all functions. Passwords can be changed at any time. The following manual shows configurations based on the admin / admin log in.*

Device Info

This section describes the system information that can be accessed using the menu items under Device Info.

Summary

Access the general status report from the router by clicking on “**Summary**” under “**Device Info**”. It shows information about the router such as software version, bootloader, etc. It also displays the current status of your DSL connection as shown below—

Device Info	
Board ID:	R4P
Software Version:	3-00-03-0400.A2pB018b2.d15h
Bootloader (CFE) Version:	1.0.37-0.7

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	800
Line Rate - Downstream (Kbps):	8000
LAN IP Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	192.168.1.1
Secondary DNS Server:	192.168.1.1

WAN

Access the WAN status report from the router by clicking on “**WAN**” under “**Device Info**”. Since a WAN connection has not been set up yet, there is no information to view. After completing the configurations for a WAN connection, you can return to this screen to view the information on your WAN status.

VPI/VCI	Con. ID	Category	Service Name	Interface Name	Protocol	IGMP	QoS	State	Status	IP Address
---------	---------	----------	--------------	----------------	----------	------	-----	-------	--------	------------

Below is how the screen will look once a WAN connection is set up.

WAN Info

VPI/VCI	Con. ID	Category	Service Name	Interface Name	Protocol	IGMP	QoS	State	Status	IP Address
3/40	1	UBR	pppoea_3_40_1	ppp_3_40_1	PPPoA	Disabled	Disabled	Enabled	Up	135.154.13.1

STATISTICS

LAN Statistics

Access the LAN statistics from the router by clicking on the “LAN” item under “Statistics”.

Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	1862	15	0	0	3266	15	0	0

Reset Statistics

WAN Statistics

Access the WAN statistics from the router by clicking on the “WAN” item under “Statistics”.

WAN Statistics

Service	VPI/VCI	Protocol	Interface	Received				Transmitted			
				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
pppoa_3_40_1	3/40	PPPoA	ppp_3_40_1	64	4	0	0	82	4	0	0
mer_3_41	3/41	MER	nas_3_41	0	0	0	0	954	3	0	0

Reset Statistics

ATM Statistics

Access ATM statistics from the router by clicking on the “ATM” item under “Statistics”.

Statistics -- ATM

ATM Interface Statistics

In Octets	Out Octets	In Errors	In Unknown	In Hec Errors	In Invalid Vpi Vci Errors	In Port Not Enable Errors	In PTI Errors	In Idle Cells	In Circuit Type Errors	In OAM RM CRC Errors	In GFC Errors
0	0	0	0	0	0	0	0	0	0	0	0

AAL5 Interface Statistics

In Octets	Out Octets	In Ucast Pkts	Out Ucast Pkts	In Errors	Out Errors	In Discards	Out Discards
0	0	0	0	0	0	0	0

AAL5 VCC Statistics

VPI/VCI	CRC Errors	SAR Timeouts	Oversized SDUs	Short Packet Errors	Length Errors

Reset Statistics

ADSL Statistics

You can view ADSL statistics by clicking on the “ADSL” item under “Statistics”. Information contained in this screen is useful for troubleshooting and diagnostics of connection problems.

- Welcome
- Device Info
 - Summary
 - WAN
 - Statistics
 - LAN
 - WAN
 - ATM
 - ADSL**
 - Route
 - ARP
- Quick Setup
- Advanced Setup
- Diagnostics
- Management

Statistics -- ADSL

Mode:	G.DMT	
Type:	Fast	
Line Coding:	Trellis On	
Status:	No Defect	
Link Power State:	LO	
	Downstream	Upstream
SNR Margin (dB):	18.9	12.0
Attenuation (dB):	0.0	1.0
Output Power (dBm):	7.8	11.9
Attainable Rate (Kbps):	11328	1108
Rate (Kbps):	8000	800
K (number of bytes in DMT frame):	251	26
R (number of check bytes in RS code word):	0	0
S (RS code word size in DMT frame):	1	1
D (interleaver depth):	1	1
Delay (msec):	0	0
Super Frames:	12703	12701
Super Frame Errors:	0	0
RS Words:	0	0
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	N/A
HEC Errors:	0	0
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	5703340	0
Data Cells:	300	0
Bit Errors:	0	0
Total ES:	0	0
Total SES:	0	0
Total UAS:	53	0

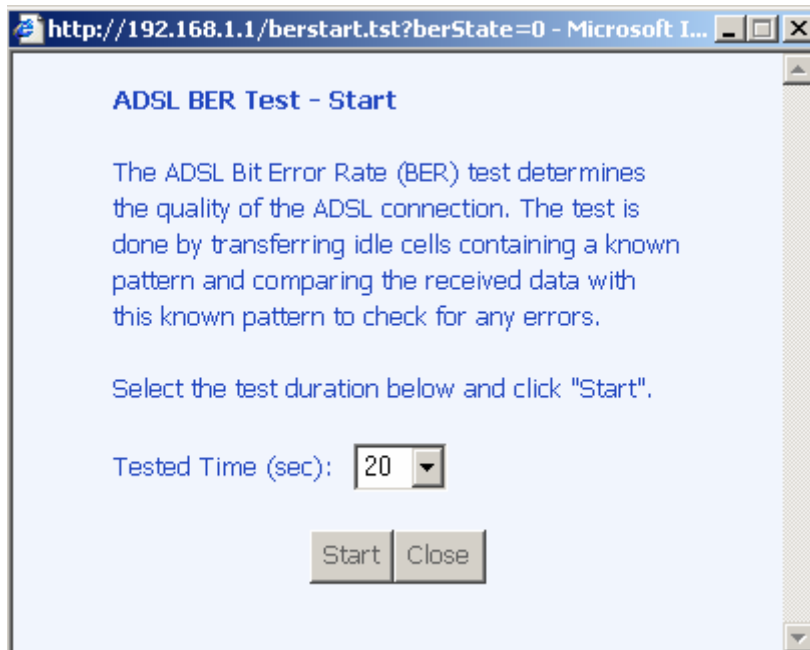
ADSL BER Test

Reset Statistics

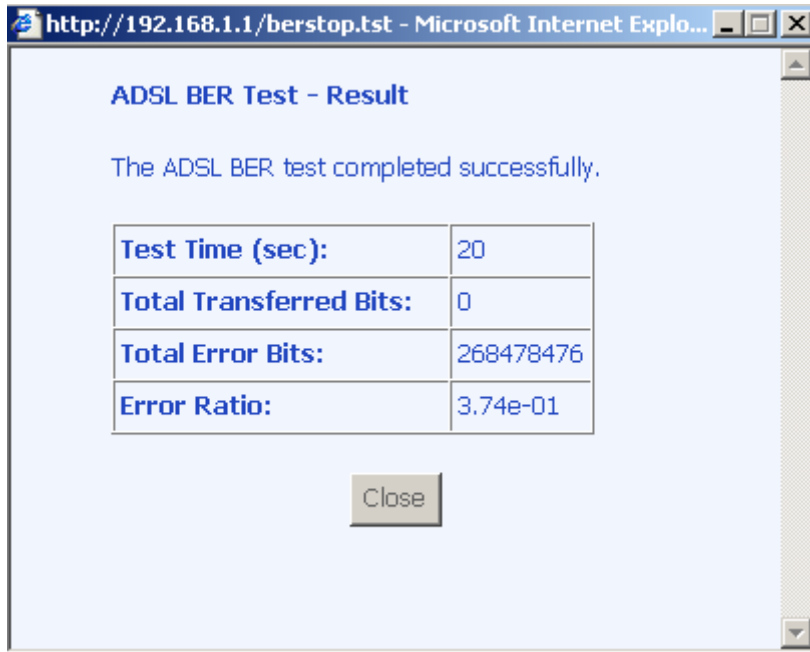
ADSL BER Test

A **Bit Error Rate Test (BER Test)** is a test that reflects the ratio of error bits to the total number transmitted.

If you click on the **ADSL BER Test** button at the bottom of the ADSL Statistics page, the following pop-up screen will appear allowing you to set the tested time and to begin the test.



Below is an ADSL BER Test result screen displaying information about the test and the error bits and ratio.



Route

Access the routing status report from the router by clicking on the “Route” item under “Device Info”.



The screenshot displays the router's configuration page. On the left is a navigation tree with 'Route' highlighted. The main content area is titled 'Device Info -- Route'. It includes a legend for flags: U - up, I - reject, G - gateway, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect). Below the legend is a table with the following data:

Destination	Gateway	Subnet Mask	Flags	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

ARP

Access the ARP status report from the router by clicking on the “ARP” item under “Device Info”.



The screenshot displays the router's configuration page. On the left is a navigation tree with 'ARP' highlighted. The main content area is titled 'Device Info -- ARP'. It includes a table with the following data:

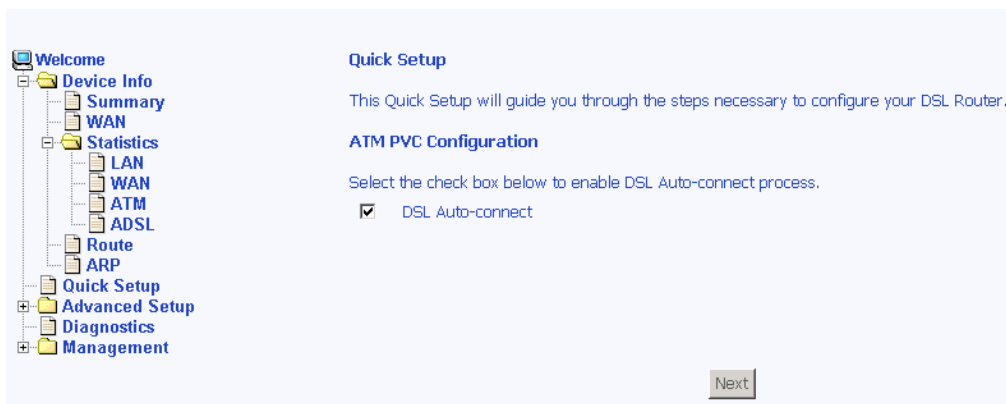
IP Address	Flags	HW Address	Device
192.168.1.177	Complete	00:08:9B:82:16:60	br0

Quick Setup

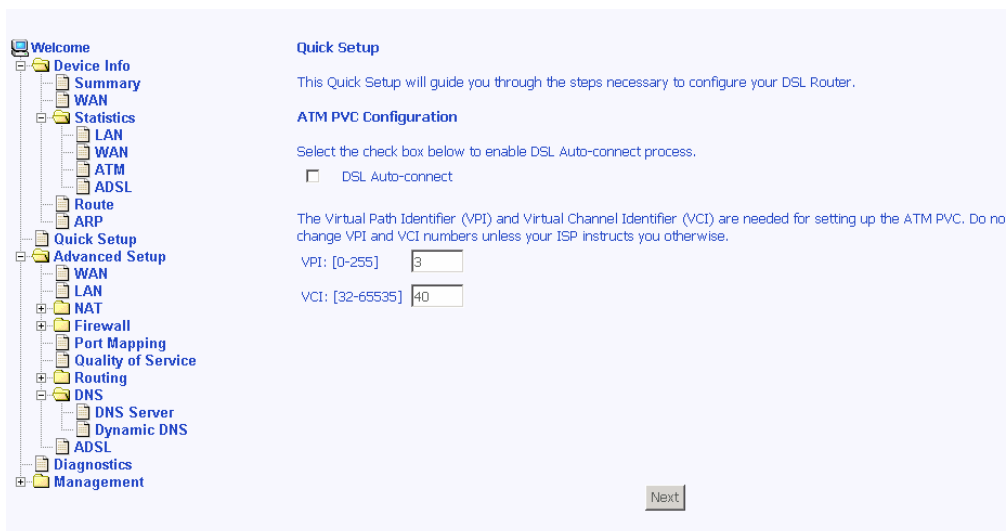
This section will explain how to configure the router for the sole purpose of connecting to the Internet.

ATM PVC Configuration

To enable the DSL auto-connect process, click on the box labeled *DSL Auto-connect*, a process that will automatically detect the first usable PVC and automatically detect PPPoE, PPPoA, and Bridge Protocol (with DHCP Server available). To continue, click on the **Next** button.



If you uncheck the *DSL Auto-connect* box, the resulting screen is seen below. Enter the VPI / VCI as indicated by your ISP and click on **Next**.



Following is the Connection Type screen where you select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use. The following is a PPPoA example. Click on **Next** to continue.

Welcome

Device Info

- Summary
- WAN
- Statistics
 - LAN
 - WAN
 - ATM
 - ADSL
- Route
- ARP

Quick Setup

Advanced Setup

- WAN
- LAN
- NAT
- Firewall
- Port Mapping
- Quality of Service
- Routing
- DNS
 - DNS Server
 - Dynamic DNS
- ADSL
- Diagnostics
- Management

Connection Type

Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use.

PPP over ATM (PPPoA)

PPP over Ethernet (PPPoE)

MAC Encapsulation Routing (MER)

IP over ATM (IPoA)

Bridging

Encapsulation Mode

VCMUX

Back Next

Enter the PPP username and password as given by your ISP. Then decide if you will be using any features such as *dial on demand*, *PPP IP extension*, *keep alive* and then click on **Next**.

Welcome

Device Info

- Summary
- WAN
- Statistics
 - LAN
 - WAN
 - ATM
 - ADSL
- Route
- ARP

Quick Setup

Advanced Setup

- WAN
- LAN
- NAT
- Firewall
- Port Mapping
- Quality of Service
- Routing
- DNS
 - DNS Server
 - Dynamic DNS
- ADSL
- Diagnostics
- Management

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username: (Do not use "<>%^[]'+\$,=#&.:)

PPP Password: (Do not use "<>%^[]'+\$,=#&.:)

Authentication Method:

Dial on demand (with idle timeout timer)

PPP IP extension

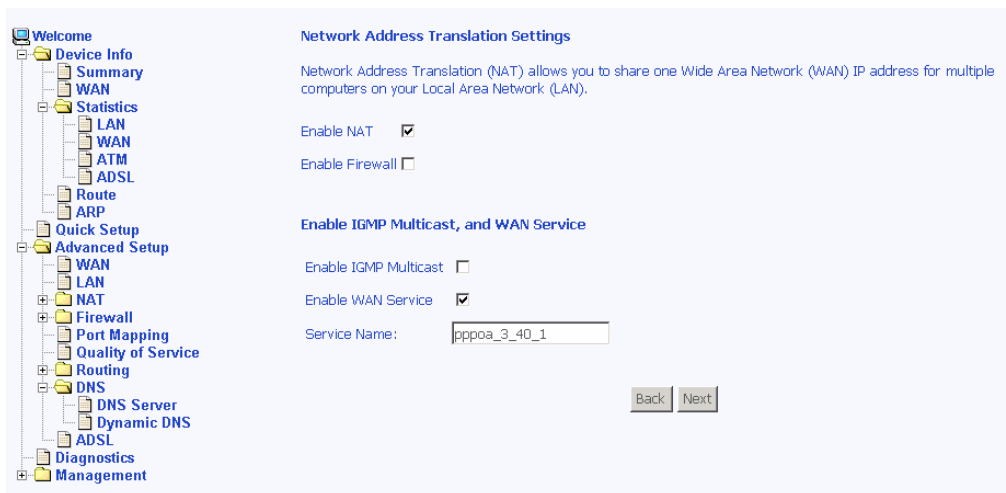
Keep Alive

Use the following default gateway:

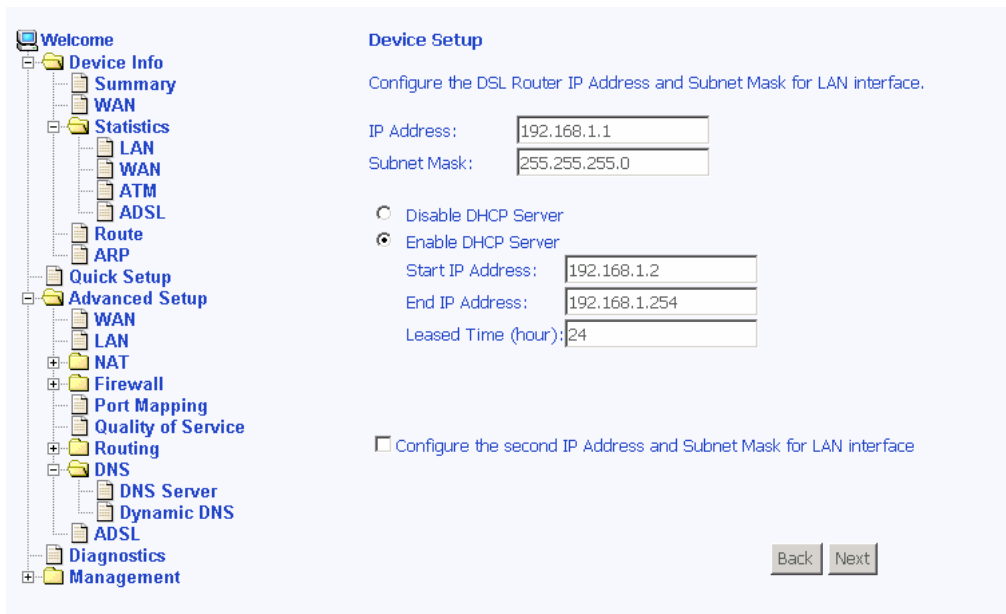
- Use IP Address:
- Use WAN Interface:

Back Next

The next step is to configure the Network Address Translation (NAT) settings. For the example, NAT will be enabled. Leave the remaining fields at default and click on **Next** to continue.



You can configure the DSL Router IP address and Subnet Mask for the LAN interface to correspond to your LAN's IP Subnet. If you want the DHCP server to automatically assign IP addresses, then enable the DHCP server and enter the range of IP addresses that the DHCP server can assign to your computers. Disable the DHCP server if you would like to manually assign IP addresses. Click on **Next** to continue.



If you have a second IP address and subnet mask for the LAN interface, click on the checkbox to configure it. See below example below.

After all of the WAN configurations have been made, the *WAN Setup Summary* screen displays all WAN settings that you have made. Check that the settings are correct before clicking on the **Save / Reboot** button. Clicking on **Save / Reboot** will save your settings and restart your router.

VPI / VCI:	3 / 40
Connection Type:	PPPoA
Service Name:	pppoa_3_40_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Advanced Setup

This section of the setup is an advanced version of the quick setup. If you want to make specific configurations to your router such as firewall, port mapping, quality of service, DNS, etc., consider going through this advanced setup for a more comprehensive configuration.

WAN

Configure the WAN settings as provided by your ISP. This section is basically the same as the Quick Setup section for configuring a WAN connection.

VPI/VCI	Con. ID	Category	Service	Interface	Protocol	IGMP	QoS	State	Remove	Edit	Action
3/40	1	UBR	pppoa_3_40_1	ppp_3_40_1	PPPoA	Disabled	Disabled	Enabled	<input type="checkbox"/>	Edit	Down
3/41	1	UBR	mer_3_41	nas_3_41	MER	Disabled	Disabled	Enabled	<input type="checkbox"/>	Edit	

Click on the **Add** button if you want to add a new rule for the WAN interface. The following ATM PVC Configuration screen appears.

VPI: [0-255] 0

VCI: [32-65535] 35

Service Category: UBR Without PCR

- UBR Without PCR
- UBR With PCR
- CBR
- Non Realtime VBR
- Realtime VBR

The ATM PVC Configuration screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category.

Verify the following values with your ISP before you change them.

- **VPI:** Virtual Path Identifier. The valid range is 0 to 255.
- **VCI:** Virtual Channel Identifier. The valid range is 32 to 65535.
- **Service Category:** Five classes of traffic are listed—
 - **UBR Without PCR** (*Unspecified Bit Rate without Peak Cell Rate*)—UBR service is suitable for applications that can tolerate variable delays and some cell losses. Applications suitable for UBR service include text/data/image transfer, messaging, distribution, and retrieval and also for remote terminal applications such as telecommuting.
 - **UBR With PCR** (*Unspecified Bit Rate with Peak Cell Rate*)--
 - **CBR** (*Constant Bit Rate*)—used by applications that require a fixed data rate that is continuously available during the connection time. It is commonly used for uncompressed audio and video information such as videoconferencing, interactive audio (telephony), audio / video distribution (e.g. television, distance learning, and pay-per-view), and audio / video retrieval (e.g. video-on-demand and audio library).
 - **Non Realtime VBR** (*Non-Real-time Variable Bit Rate*)—can be used for data transfers that have critical response-time requirements such as airline reservations, banking transactions, and process monitoring.
 - **Realtime VBR** (*Real-time Variable Bit Rate*)—used by time-sensitive applications such as real-time video. Rt-VBR service allows the network more flexibility than CBR.

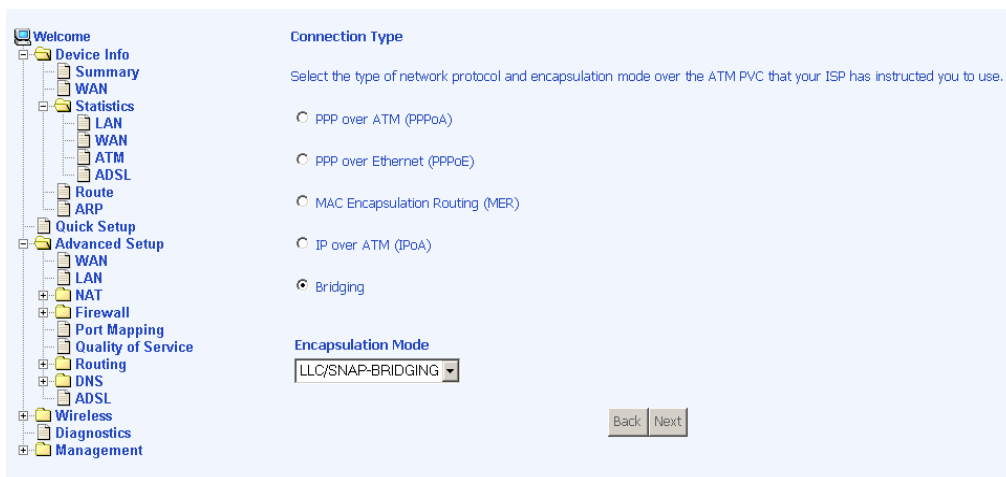
Enabling QoS for a PVC improves performance for selected classes of applications. However, since QoS also consumes system resources, the number of PVCs is reduced. If you want to enable QoS service, click on the **Enable Quality Of Service** check box.

Connection Type

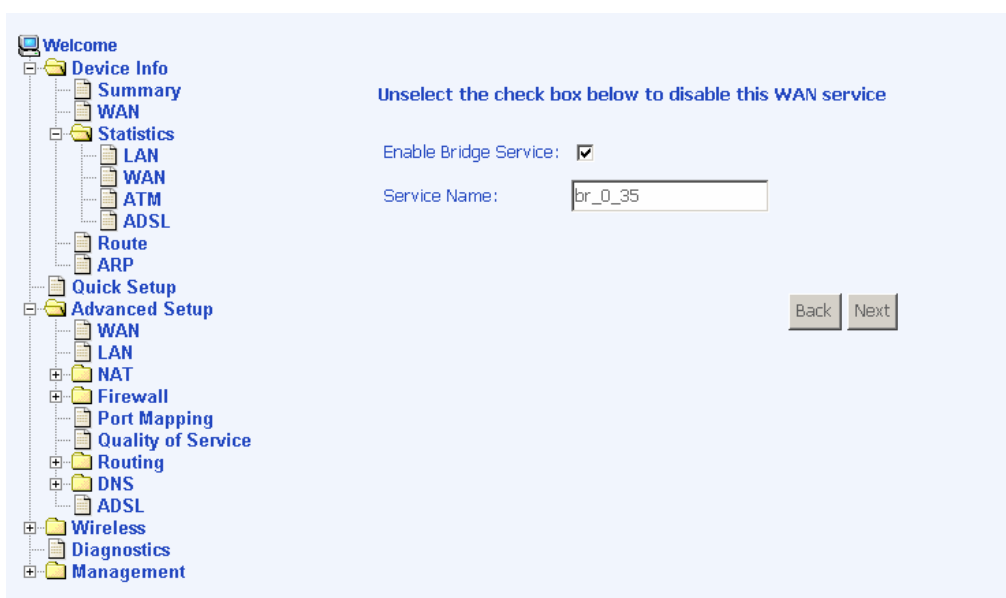
This screen shows the below types of network protocols and encapsulation modes—

- PPP over ATM (PPPoA)
- PPP over Ethernet (PPPoE)
- MAC Encapsulation Routing (MER)
- IP over ATM (IpoA)
- Bridging

Select the mode that your ISP has instructed you to use and click on **Next**. The example below is a *bridge connection type*.



After you click on **Next**, the below screen appears allowing you to disable the bridge service if desired.



When the settings are complete, the next screen shows a **WAN Setup - Summary** screen displaying the WAN configurations made.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

VPI / VCI:	0 / 35
Connection Type:	Bridge
Service Name:	br_0_35
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Disabled

Click "Save" to save these settings. Click "Back" to make any modifications.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

Back Save

After the settings are saved, the below screen will follow, displaying the WAN settings that you made with the option to **Add** or **Remove** any of the connections that you have made. When satisfied with the settings click on the **Finish** button.

WAN Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Finish to apply the changes and reboot the system.

VPI/VCI	Con. ID	Category	Service	Interface	Protocol	IGMP	QoS	State	Remove	Edit	Action
0/35	1	UBR	br_0_35	nas_0_35	Bridge	N/A	Disabled	Enabled	<input type="checkbox"/>	Edit	

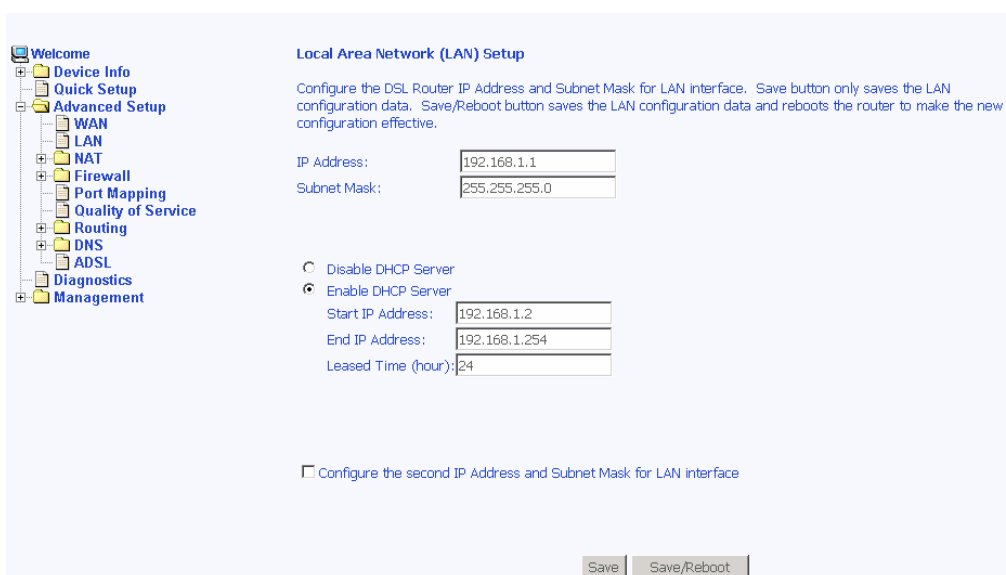
Add Remove Finish

After selecting the **Finish** button, the below screen will appear. At this point, the router will reboot to save the changes made.



LAN Local Area Network (LAN) Setup

You can configure the DSL Router IP address and Subnet Mask for the LAN interface to correspond to your LAN's IP Subnet. If you want the DHCP server to automatically assign IP addresses, then enable the DHCP server and enter the range of IP addresses that the DHCP server can assign to your computers. Disable the DHCP server if you would like to manually assign IP addresses. Click on **Next** to continue. The **Save** button only saves the LAN configuration data, but does not apply the configurations. Select the **Save/Reboot** button to save the LAN configuration data and reboot the router and apply the new configurations.



NAT

If you enable NAT (Network Address Translation), you can configure the Virtual Server, Port Triggering, and DMZ Host.

Virtual Servers

A virtual server allows you to direct incoming traffic from the WAN side to a specific IP address on the LAN side. Click on the **Add** button to set up a virtual server.

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side(identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. Maximum 32 entries can be configured.

Add

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	--------

In the next screen, select the virtual server from the drop-down list and complete the server IP address, then click on the **Save / Apply** button.

The following screen appears after you save your selection. To add additional virtual servers, click on the **Add** button. If you need to remove any of the server names, select the check box and click on the **Remove** button.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove
Active Worlds	3000	3000	TCP	3000	3000	192.168.1.100	<input type="checkbox"/>
Active Worlds	5670	5670	TCP	5670	5670	192.168.1.100	<input type="checkbox"/>
Active Worlds	7777	7777	TCP	7777	7777	192.168.1.100	<input type="checkbox"/>
Active Worlds	7000	7000	TCP	7000	7000	192.168.1.100	<input type="checkbox"/>

Port Triggering

Click on the **Add** button to add Port Triggering to your Internet application.

NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. Maximum 32 entries can be configured.

Add

Application	Trigger		Open		Remove	
	Name	Protocol	Port Range	Protocol		Port Range
			Start End		Start End	

The below screen appears when you click on **Add** allowing you to select the application that you want to set the port settings for. After a selection has been made, click on the **Save / Apply** button.

NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it. **Remaining number of entries that can be configured:32**

Application Name:

Select an application:

Custom application:

Save/Apply

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Save/Apply

The below screen appears after you save your selections showing the name of the application that you have added a port triggering function. You will be able to add or remove selections made, by clicking on the **Add** and **Remove** buttons.

NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. Maximum 32 entries can be configured.

Add Remove

Application	Trigger		Open		Remove	
	Name	Protocol	Port Range	Protocol		Port Range
			Start End		Start End	
Aim Talk		TCP	4099 4099	TCP	5191 5191	<input type="checkbox"/>

DMZ Host

You can define the IP address of the DMZ Host on this screen. Enter the IP address and click on **Save / Apply**.

NAT -- DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ Host IP Address:

Save/Apply

Firewall

IP Filtering—Outgoing

The outgoing filter will block LAN traffic from entering the WAN side. Click on the **Add** button to create filters.



The below screen will appear when you click on **Add**. Input the filter name, source information (from the LAN side), and destination information (from the WAN side). Then click on **Save / Apply**.



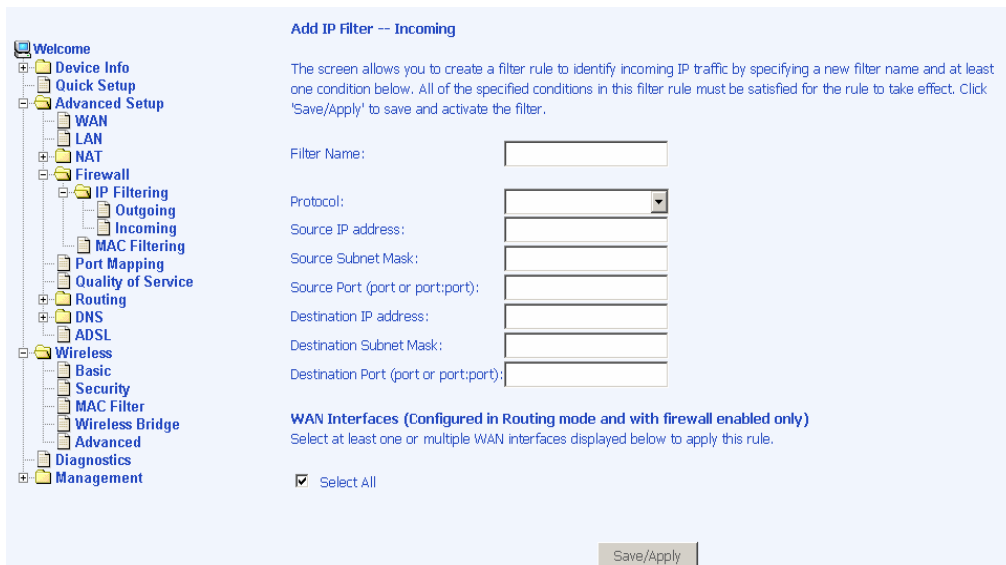
IP Filtering—Incoming

Incoming filter filters the WAN traffic to the LAN side. Click on the **Add** button to add incoming filter settings.



The screenshot shows the 'Incoming IP Filtering Setup' page. On the left is a navigation tree with 'Incoming' highlighted under 'IP Filtering'. The main content area has a title 'Incoming IP Filtering Setup' and a paragraph: 'By default, all incoming IP traffic from WAN is blocked when firewall is enabled, but some IP traffic can be **ACCEPTED** by setting up filters.' Below this is a table with the following columns: Name, VPI/VCI, Protocol, Source Address / Mask, Source Port, Dest. Address / Mask, Dest. Port, and Remove. An 'Add' button is located below the table.

Enter a filter name, information about the source address (from the WAN side), and information about the destination address (to the LAN side). Select the protocol and WAN interface, and then click on **Save/Apply** to add the setting.



The screenshot shows the 'Add IP Filter -- Incoming' page. On the left is the same navigation tree. The main content area has a title 'Add IP Filter -- Incoming' and a paragraph: 'The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.' Below this are several form fields: 'Filter Name:' (text input), 'Protocol:' (dropdown menu), 'Source IP address:' (text input), 'Source Subnet Mask:' (text input), 'Source Port (port or port:port):' (text input), 'Destination IP address:' (text input), 'Destination Subnet Mask:' (text input), and 'Destination Port (port or port:port):' (text input). Below these fields is a section titled 'WAN Interfaces (Configured in Routing mode and with firewall enabled only)' with a paragraph: 'Select at least one or multiple WAN interfaces displayed below to apply this rule.' There is a checked checkbox labeled 'Select All'. At the bottom right is a 'Save/Apply' button.

MAC Filtering

MAC filtering can forward or block traffic by MAC address. You can change the policy or add settings to the MAC filtering table using the MAC Filtering Setup screen.

MAC Filtering Setup

MAC Filtering Global Policy: **FORWARDED**

Change Policy

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

Choose Add or Remove to configure MAC filtering rules.

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
---------	----------	-----------------	------------	-----------------	--------

Add

If you click on **Change Policy**, a confirmation dialog appears, allowing you to verify your change.

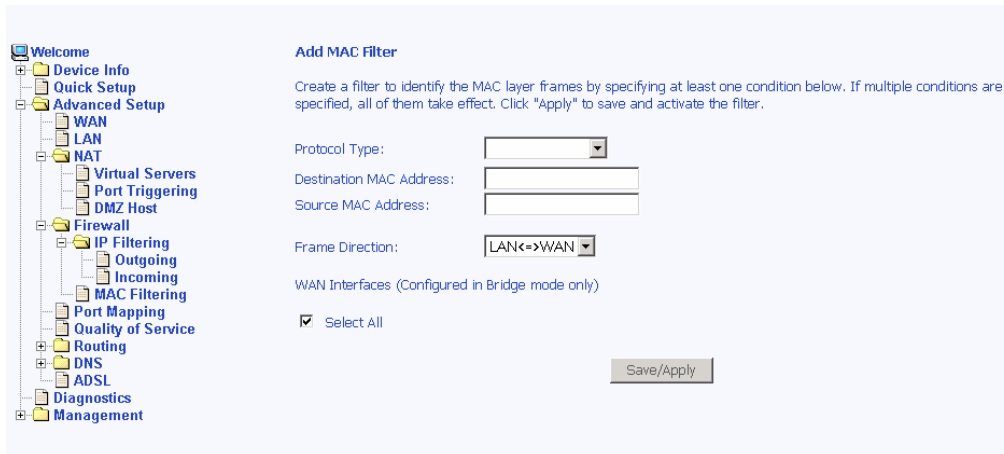
Change MAC Filtering Global Policy

WARNING: Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Are you sure you want to change MAC Filtering Global Policy from **FORWARDED** to **BLOCKED** ?

NO YES

If you want to add a setting to the MAC filtering table, enter the Source and Destination MAC address, and select protocol type, frame direction, and WAN interface. Then click on **Save / Apply** to save it.

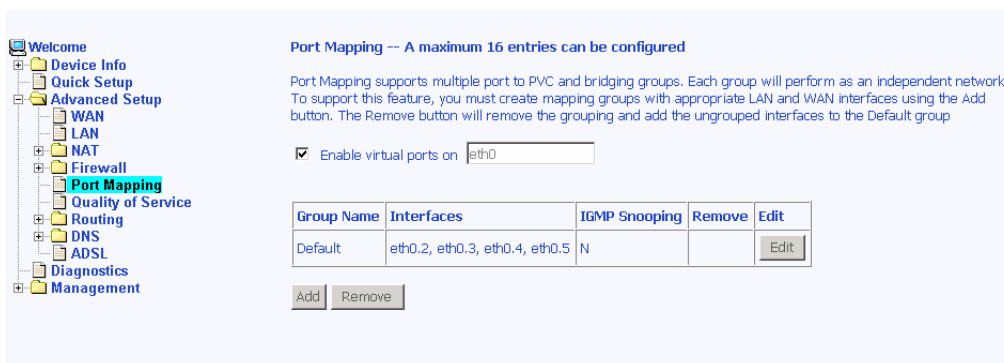


After you save the settings, a screen showing the settings will appear. On this screen you will be able to view and delete MAC filtering rules.

Port Mapping

Port mapping is a feature that allows you to open ports to allow certain Internet applications on the WAN side to pass through the firewall and enter your LAN. To use this feature, mapping groups need to be created. To do this, follow the below instructions—

1. Click on the **Add** button as displayed below.



2. If you need to edit an entry, then click on the **Edit** button.

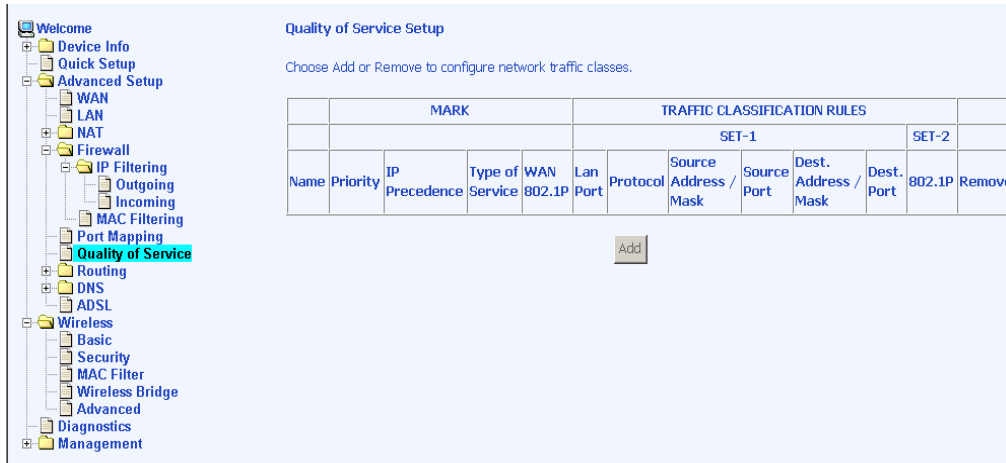


After clicking the **Add** button, the below configuration screen appears, allowing you enter the groups and the interfaces they are associated with.



Quality of Service

You can configure the Quality of Service to apply different priorities to traffic on the router. Click on **Add** to view the *Add Network Traffic Class Rule* screen.



This screen allows you to add a network traffic class rule. Procedures for this setup are as follows—

1. Give a name to this traffic class.
2. Assign a priority level—low, medium, and high—to this traffic class.
3. Select an IP precedence from the range of 0-7.
4. Enter an IP Type of Service from the following selections—
 - Normal Service
 - Minimize Cost
 - Maximize Reliability
 - Maximize Throughput
 - Minimize Delay
5. Last, enter the traffic conditions for the class such as the protocol (TCP / UDP, TCP, UDP, or ICMP) to be used. Click **Save / Apply** to save the settings.

Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.

Traffic Class Name:

Assign Priority and/or IP Precedence and/or Type Of Service for the class
 If non-blank value is selected for 'IP Precedence' and/or 'IP Type Of Service', the corresponding TOS byte in the IP header of the upstream packet will be overwritten by the selected value.

Priority:

IP Precedence:

IP Type Of Service:

Specify Traffic Conditions for the class
 Enter the following conditions either for IP layer or for the IEEE 802.1p priority.

Protocol:

Source IP Address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP Address:

Destination Subnet Mask:

Destination Port (port or port:port):

802.1p Priority:

Routing

Default Gateway

You can enable automatic assigned default gateway on the Routing - Default Gateway screen. As default, the box is checked for automatic assigned default gateway to be enabled. Click the **Save / Apply** button to enable or disable this feature.

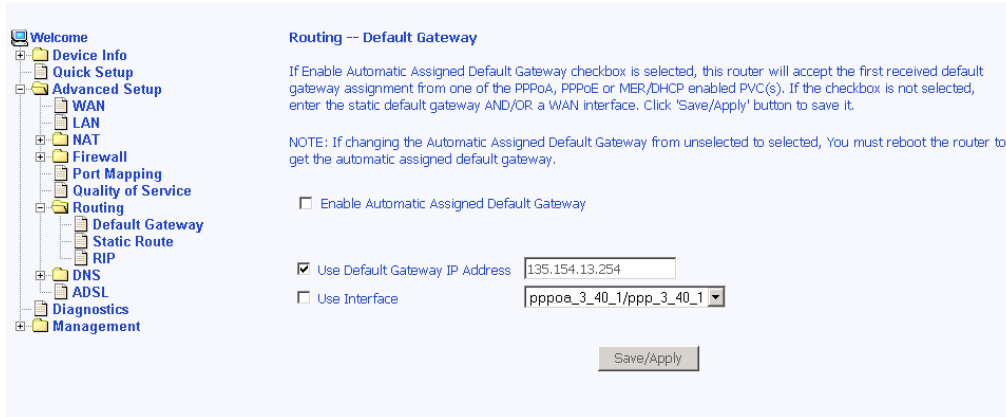
Routing -- Default Gateway

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

Enable Automatic Assigned Default Gateway

If you do not want to enable *Automatic Assigned Default Gateway*, then uncheck the box as seen below. You will be given the choice to use the default gateway IP address. If you decide to change the automatic assigned default gateway address, you must reboot the router to be assigned a new default gateway IP address. Also, select the WAN interface that you will be using. Click on **Save / Apply** to save the settings.



Static Route

Use the Routing - Static Route screen to add a static route to the routing table.

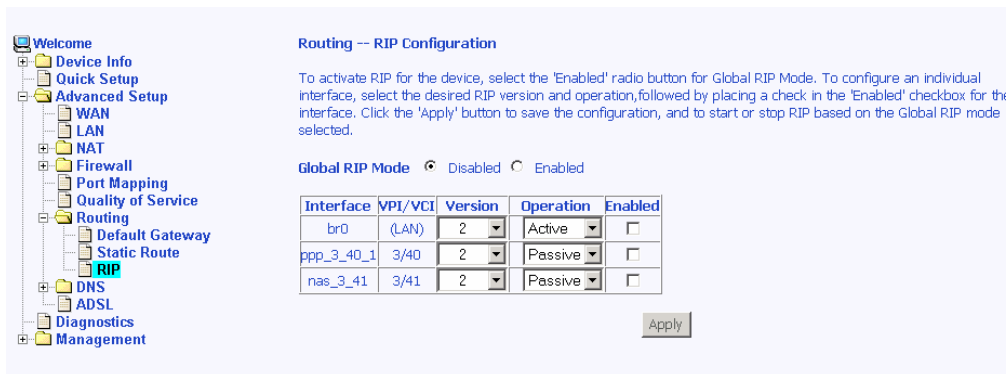


Enter the route information and click on **Save/Apply** to make it active. No reboot is required.



RIP

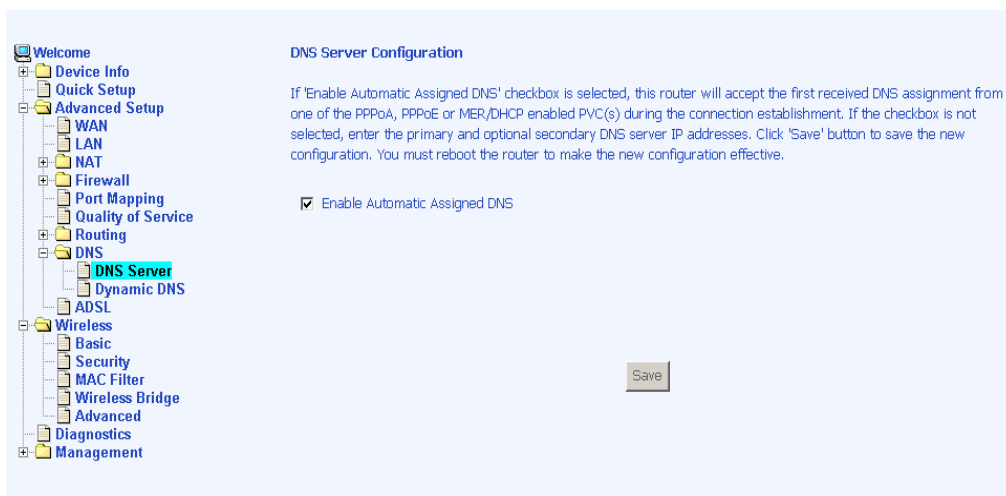
If RIP is enabled, the router operation can be configured as active or passive.



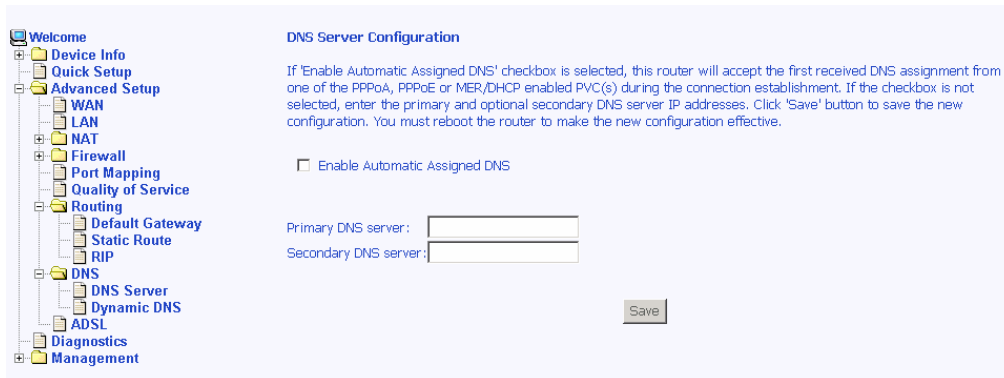
DNS

DNS Server

Use the DNS Server screen to request automatic assignment of a DNS or to specify a primary and secondary DNS.

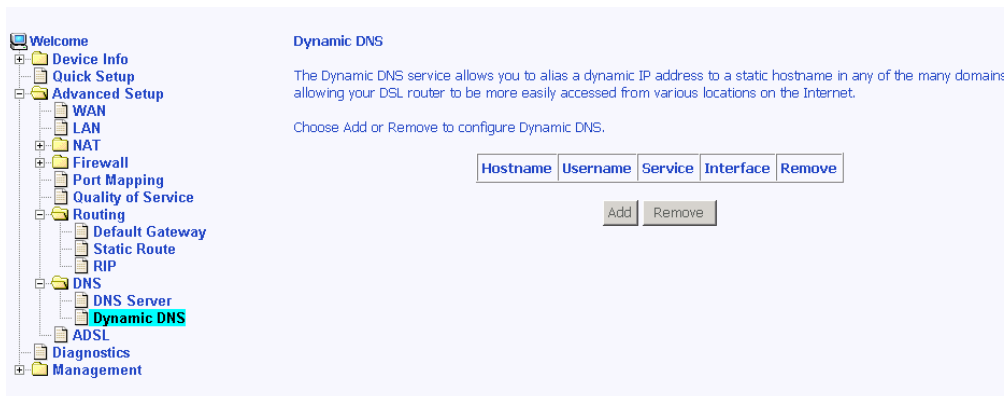


If you uncheck the *Enable Automatic Assigned DNS* checkbox, then there will be two additional fields—primary and secondary DNS server—to enter as seen below.



Dynamic DNS

Dynamic DNS is a service for allowing an Internet domain name to be assigned to a varying IP address. This makes it possible for other sites on the Internet to establish connections to your without needing to track the IP address themselves. Click on **Add** to set up a dynamic DNS configuration.



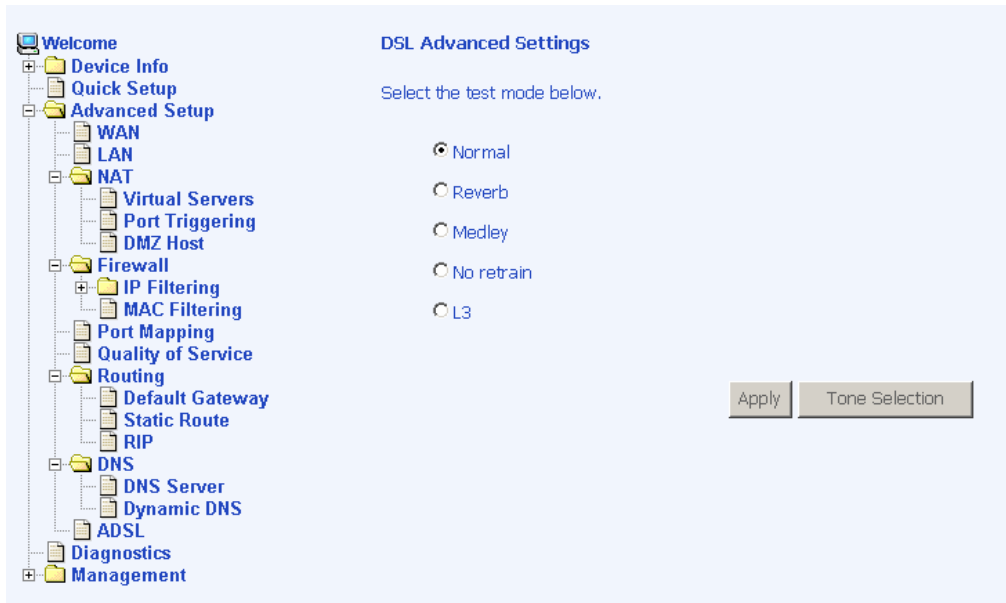
This screen allows you to add a dynamic DNS address from DynDNS.org or TZO. Enter the hostname and the interface that you are using. Also enter the username and password assigned by the DNS service. Click on **Save / Apply** to save these configurations.

ADSL

The DSL settings page contains three sections—modulation, phone line, and capability—that should be specified by your ISP. Consult with your ISP to select the correct settings for each. Then click on **Save / Apply** if you are finished or click on **Advanced Settings** if you want to configure more advanced settings.

DSL Advanced Settings

The test mode can be selected from the DSL Advanced Settings page. Test modes include—normal, reverb, medley, no retrain, and L3. After you make your selections of the test mode, click on **Apply** to save these settings first before you go to *Tone Selection*.



Tone Settings

The frequency band of ADSL is split up into 256 separate tones, each spaced 4.3125 kHz apart. With each tone carrying separate data, the technique operates as if 256 separate modems were running in parallel. The tone range is from 0 to 31 for upstream and from 32 to 255 for downstream. Do not change these settings unless so directed by your ISP.

ADSL Tone Settings

Upstream Tones

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Downstream Tones

32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47
 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79
 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95
 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111
 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127
 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143
 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159
 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175
 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191
 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207
 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223
 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239
 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255

Check All Clear All Apply Close

Diagnostics

The diagnostics screen allows you to run diagnostic tests to check your DSL connection. The results will show test results of three connections—

- Connection to your local network
- Connection to your DSL service provider
- Connection to your Internet service provider

There are two buttons at the bottom of the page—**Test** and **Test with OAM F4**—which will allow you to retest if necessary.

The screenshot shows the 'pppoa_3_40_1 Diagnostics' page. On the left is a navigation menu with items like Welcome, Device Info, Quick Setup, Advanced Setup, Diagnostics (highlighted), Management, Settings, System Log, SNMP, Internet Time, Access Control, Update Software, and Reboot Router. The main content area has a title 'pppoa_3_40_1 Diagnostics' and a paragraph explaining that the modem can test the DSL connection. Below this are three sections of test results, each with a table of test names, results, and help links.

Test the connection to your local network

Test your Ethernet Connection:	PASS	Help
--------------------------------	------	----------------------

Test the connection to your DSL service provider

Test ADSL Synchronization:	PASS	Help
Test ATM OAM F5 segment ping:	PASS	Help
Test ATM OAM F5 end-to-end ping:	PASS	Help

Test the connection to your Internet service provider

Test PPP server session:	PASS	Help
Test authentication with ISP:	PASS	Help
Test the assigned IP address:	PASS	Help
Ping default gateway:	PASS	Help
Ping primary Domain Name Server:	PASS	Help

At the bottom of the page are three buttons: 'Next Connection', 'Test', and 'Test With OAM F4'.

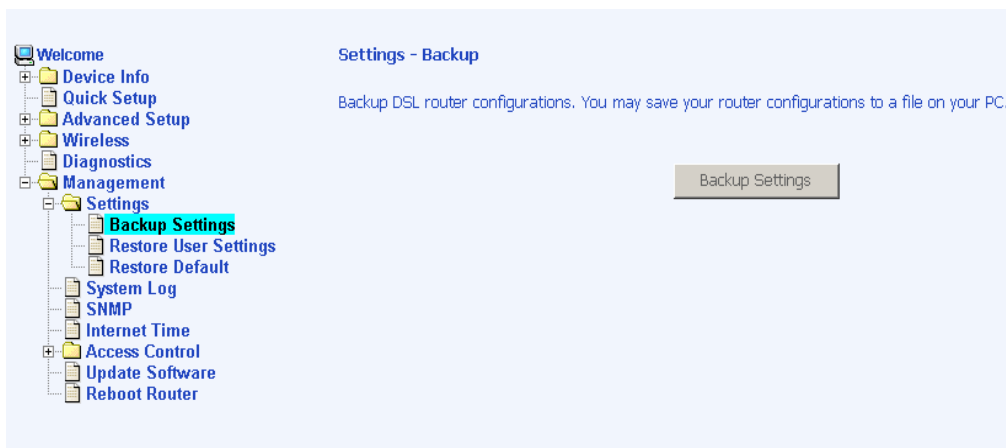
Management

The Management section gives you access to certain setups for the purpose of maintaining the system, including backing up the configurations, viewing system log, maintaining access control, updating software, etc.

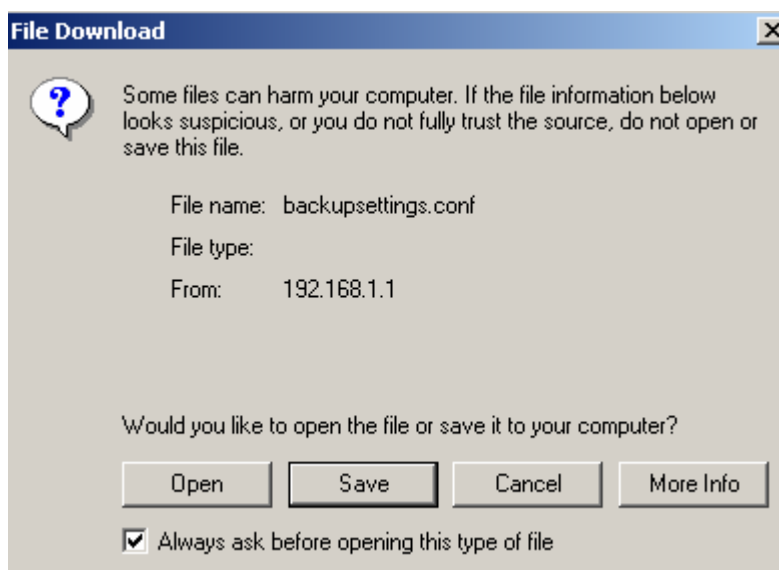
Settings

Backup Settings

To save a copy of the configurations that you have made on your router, click on the **Backup Settings** button.



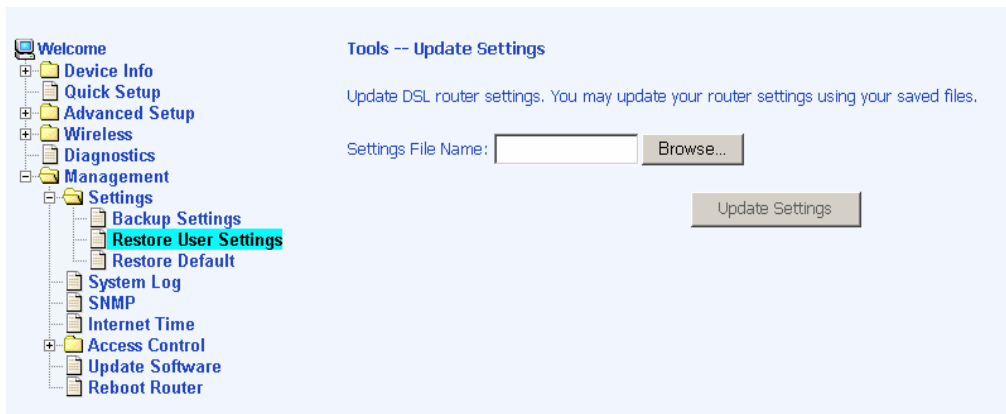
The below pop-up screen will appear with a prompt to open or save the file to your computer.



Restore User Settings

To restore saved settings, select Management→Settings→Restore User Settings.

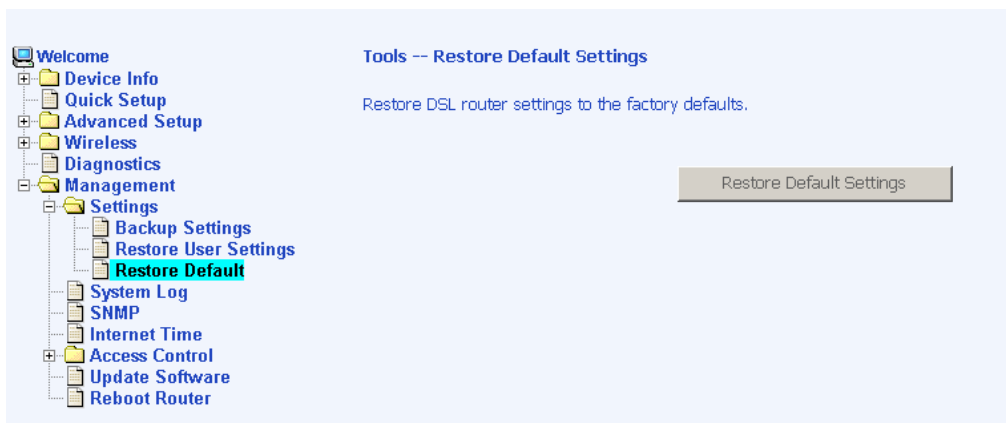
Select the backup file you want to restore and click on **Update Settings**.



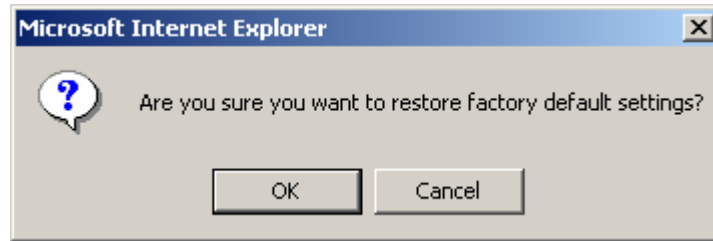
The router will restore settings and reboot to activate the restored settings.

Restore Default

Restore Default will delete all current settings and restore the router to factory default settings. To restore the router to factory default settings, select Management→Settings→Restore Default. Click on the **Restore Default Settings** button.



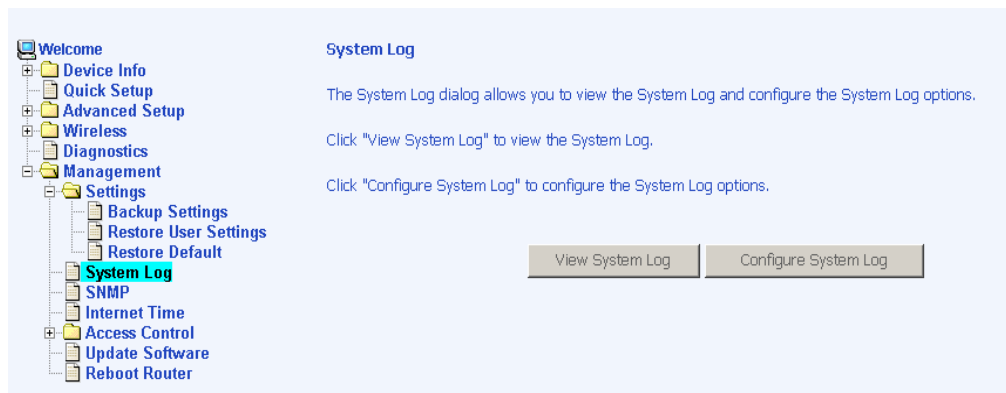
Click on **OK** when the pop-up window appears confirming that you want to restore factory default settings to your router.



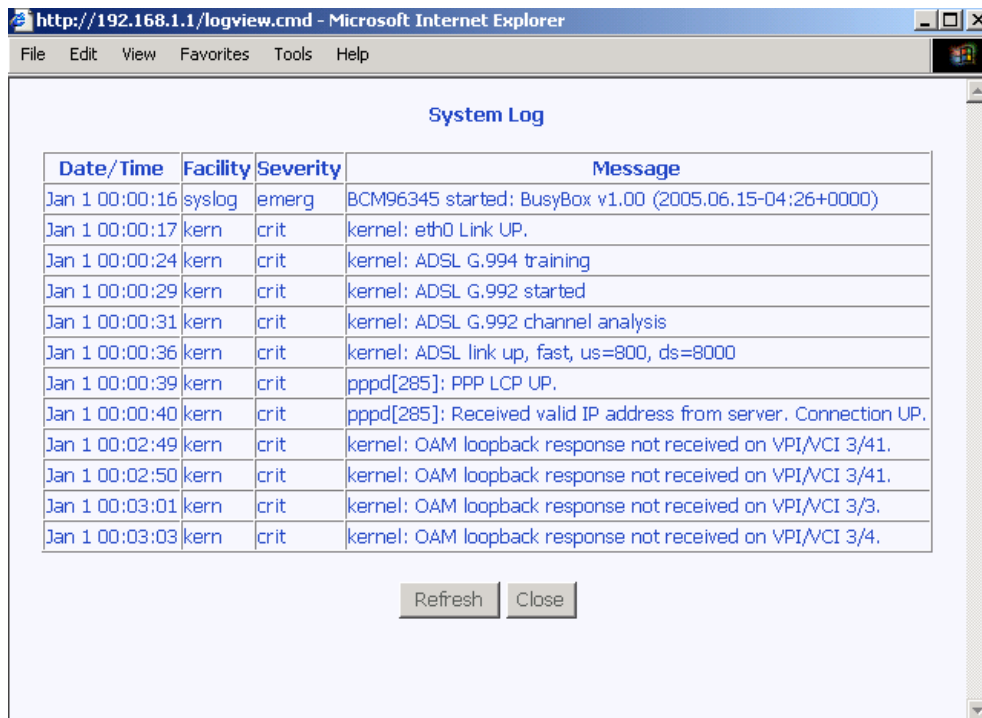
The router will restore the default settings and reboot.

System Log

The System Log dialog allows you to view the System Log and configure the System Log options. To view the System Log click on the **View System Log** button to check the log file.

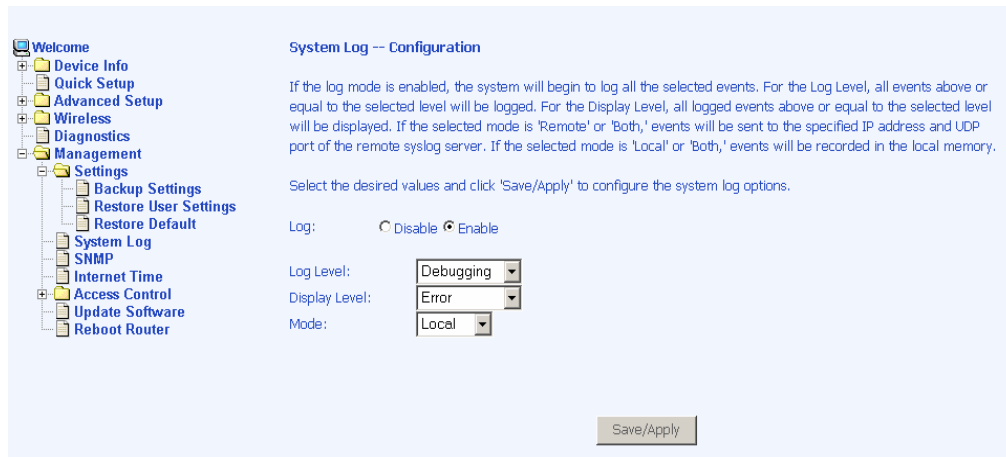


Below is a view of the System Log.



Configure System Log

If the log is enabled, the system will log selected events: Emergency, Alert, Critical, Error, Warning, Notice, Informational, and Debugging. All events above or equal to the selected log level will be logged and displayed.

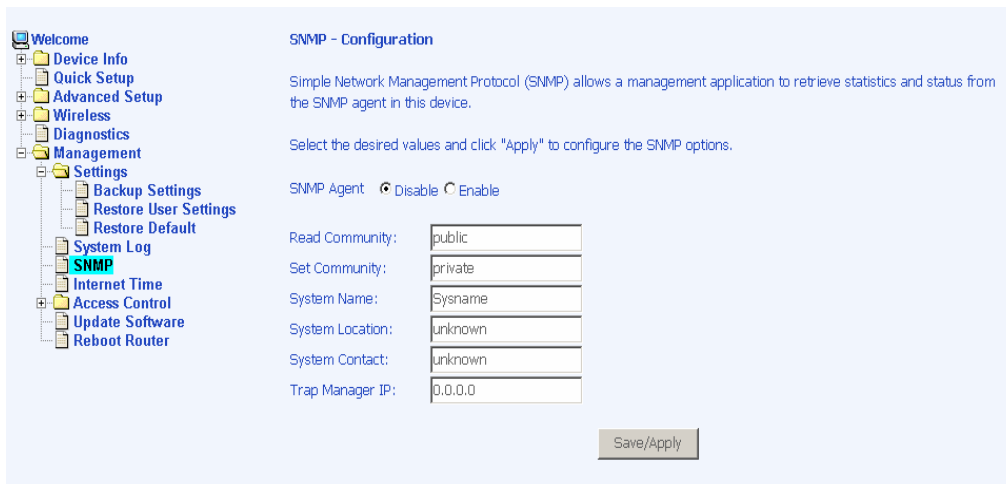


The screenshot shows a web interface for configuring system logs. On the left is a navigation tree with categories like Welcome, Device Info, Quick Setup, Advanced Setup, Wireless, Diagnostics, Management, and Settings. Under Settings, 'System Log' is selected. The main content area is titled 'System Log -- Configuration'. It contains explanatory text about logging levels and modes, followed by configuration options: 'Log' (radio buttons for Disable and Enable, with Enable selected), 'Log Level' (dropdown menu set to Debugging), 'Display Level' (dropdown menu set to Error), and 'Mode' (dropdown menu set to Local). A 'Save/Apply' button is at the bottom right.

If the selected mode is “Remote” or “Both”, events will be sent to the specified IP address and UDP port of a remote system log server. If the selected mode is “Local” or “Both”, events will be recorded in the local memory. Select the desired values and click on the “**Save/Apply**” button to configure the system log options.

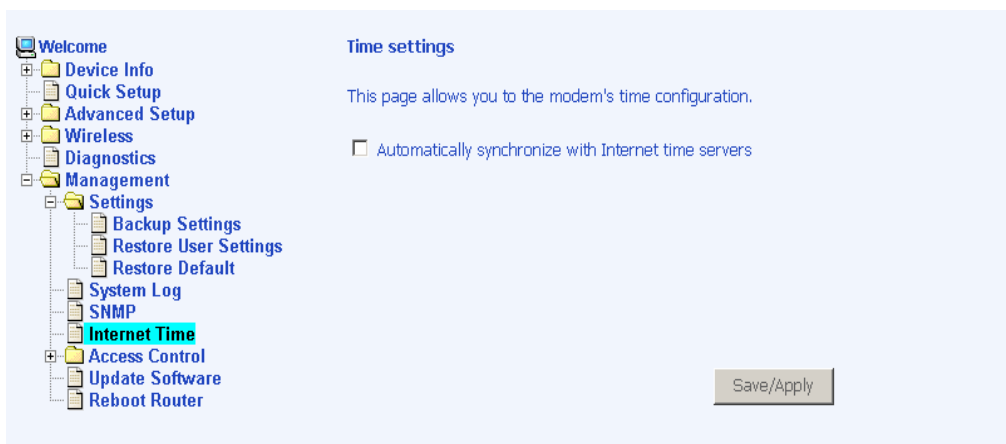
SNMP

SNMP is Simple Network Management Protocol that provides a means to monitor status and performance as well as set configuration parameters. It enables a management station to configure, monitor and receive trap messages from network devices.



Internet Times

The Time Settings page allows you to automatically synchronize your time with a timeserver on the Internet.



If you choose to automatically synchronize with Internet time servers, then click on the box and the below fields appear. Select from the list of NTP (Network Time Protocol) time servers. Then select the time zone that you are in and click on **Save / Apply** to save and complete your time settings.

Time settings

This page allows you to the modem's time configuration.

Automatically synchronize with Internet time servers

First NTP time server:

Second NTP time server:

Time zone offset:

Access Control

You can enable or disable some services of your router by LAN or WAN. If no WAN connection is defined, only the LAN side can be configured.

Services

Service	LAN	WAN
FTP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
HTTP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
ICMP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
SNMP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
SSH	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
TELNET	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
TFTP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled

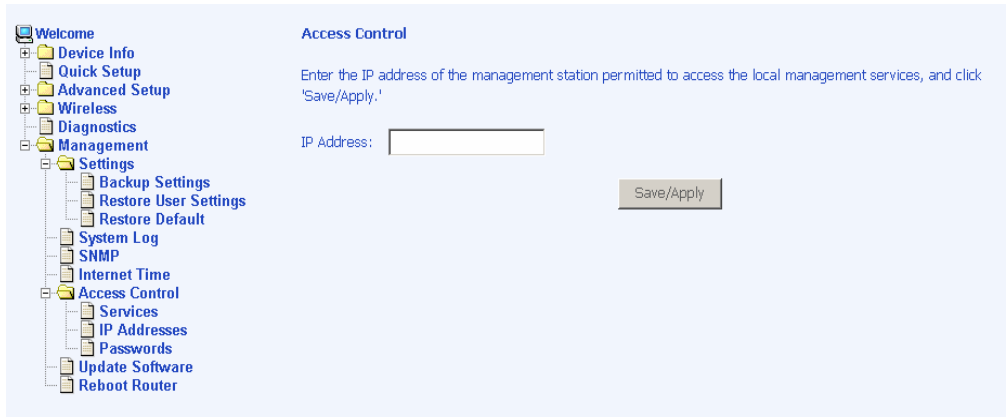
IP Addresses

Web access to the router can be limited when Access Control Mode is enabled. The IP addresses of allowed hosts can be added using Access Control→IP Address.

Add the IP address to the IP address list by clicking on the **Add** button, then select **“Enabled”** to enable Access Control Mode.

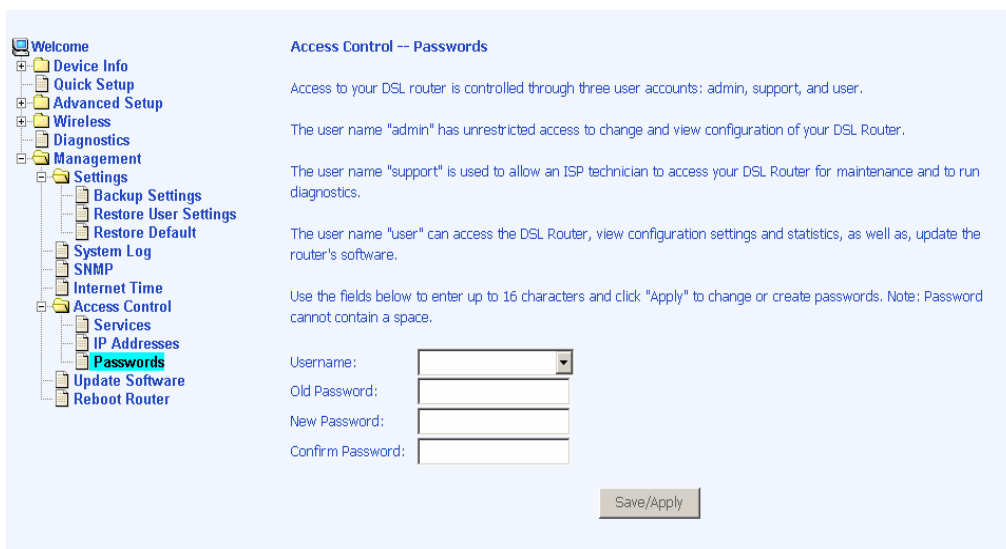
Access Control Mode Disabled Enabled

To assign the IP address of the management station that is permitted to access the local management services, enter the IP address in the box and click on the **Save / Apply** button.



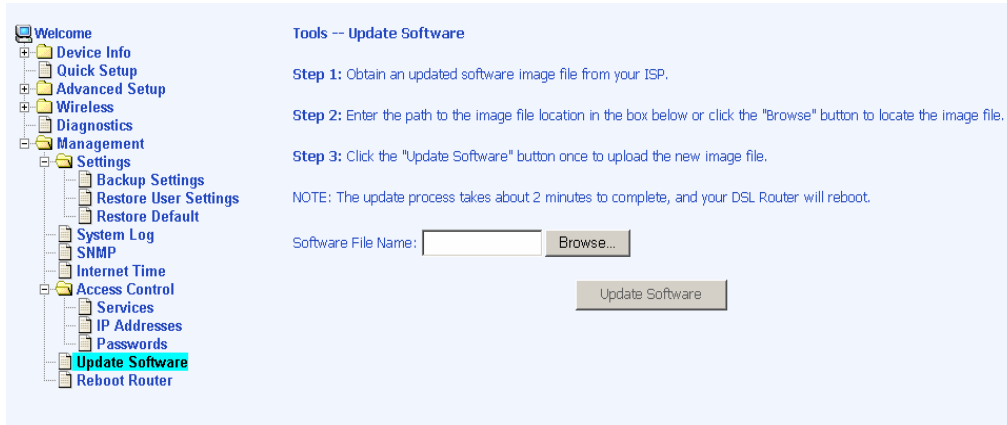
Passwords

Access the **Passwords** screen under the **Access Control** section to change a password. Select an account and enter the current password and the new password and then click on the **Save / Apply** button.



Update Software

If your ISP releases new software for this router, follow the below steps to perform an upgrade.



Tools -- Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

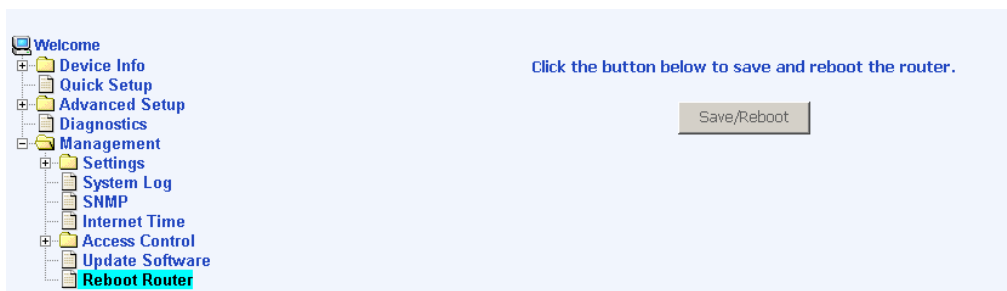
Step 3: Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

Software File Name:

Reboot Router

Select Management→Reboot Router to reboot the router using the web interface. The router will save the current configuration and reboot itself using the new configuration.



Click the button below to save and reboot the router.